The invention in which an exclusive right is claimed is defined by the following:

1. A method for ensuring that data stored in a persistent storage of a client computing device have not been modified when the data are subsequently accessed for use by the client computing device, comprising the steps of:

(a) employing a key that is only known and available for use by a server computing device to compute a signature for the data before the data are stored in the persistent storage by the client computing device;

(b) storing the signature and the data in the persistent storage of the client computing device;

(c) before the data are subsequently used by the client computing device, as a function of the signature and of the data that were stored, verifying that the data that were stored have not been changed; and

(d) only using the data that were stored if the step of verifying indicates that the data that were stored have not been changed since the signature was computed before storing the data and the signature.

2. The method of Claim 1, wherein the step of employing the key comprises the step of sending the data from the client computing device to the server computing device so that the server computing device computes the signature for the data and sends the signature back to the client.

3. The method of Claim 1, wherein the step of verifying comprises the steps of:

(a) sending the data and the signature that were stored from the client computing device to the server computing device;

(b) using the key, computing a temporary signature for the data that were stored; and

(c) comparing the temporary signature with the signature to determine a result, said result indicating that the data that were stored have been altered, if the temporary signature is different than the signature.

4. The method of Claim 3, further comprising the step of sending the result from the server computing device to the client computing device.

5. The method of Claim 1, wherein the step of employing the key comprises the steps of:

(a) computing a digest of the data before the data are stored in the persistent storage;

(b) on the server computing device, computing the signature of the digest using the key; and

(c) sending the signature from the server computing device to the client computing device for storage in the persistent storage.

6. The method of Claim 5, wherein the step of verifying comprises the steps of:

(a) computing a temporary digest of the data that were stored;

(b) sending the temporary digest and the signature from the client computing device to the server computing device;

(c) on the server computing device, using the key for computing a temporary signature of the temporary digest; and

(d) comparing the temporary signature with the signature to determine a result, said result indicating the data that were stored have been altered, if the temporary signature is different than the signature.

7. The method of Claim 6, further comprising the step of sending the result from the server computing device to the client computing device.

8. The method of Claim 5, further comprising the steps of:

(a) obtaining a signer identification (ID) for the client computing device, the signer (ID) uniquely indicating the client computing device and not being controlled by an operator of the client computing device;

(b) concatenating the signer ID with the digest before computing the signature on the server computing device; and

(c) storing the signer ID and the signature in the persistent storage of the client.

9. The method of Claim 8, wherein the step of verifying comprises the steps of:

(a) computing a temporary digest of the data that were stored;

(b) sending the signer ID, the signature, and the temporary digest of the data to the server;

(c) concatenating the signer ID and the temporary digest;

(d) on the server computing device, using the key for computing a temporary signature for the signer ID and the temporary digest that were concatenated; and

(e) comparing the temporary signature with the signature to determine a result, said result indicating that the data that were stored have been altered or the signer ID has been changed, if the temporary signature is different than the signature.

10. The method of Claim 9, further comprising the step of sending the result from the server computing device to the client computing device.

11. The method of Claim 1, wherein the data comprise a plurality of different sets of data, further comprising the steps of:

(a) obtaining a signer identification (ID) for the client computing device, the signer ID uniquely indicating the client computing device and not being controlled by an operator of the client computing device;

(b) on the server computing device, using the key for computing an intermediate key from a concatenation of an arbitrary value and the signer ID;

(c) sending the intermediate key from the server computing device to the client computing device;

(d) using the intermediate key to sign each set of the data to produce the signature for the set of data; and

(e) storing the signature, the arbitrary value, and the signer ID on the persistent storage.

12. The method of Claim 11, wherein the step of verifying comprises the steps of:

(a) computing a temporary digest of a set of the data that were stored;

(b) sending the temporary digest, and the arbitrary value and the signer ID that were stored, from the client computing device to the server computing device;

(c) on the server computing device, using the key for computing a temporary intermediate key from a concatenation of the arbitrary value and the signer ID;

(d) using the temporary intermediate key, computing a temporary signature for the temporary digest; and

(e) comparing the temporary signature with the signature to determine a result, said result indicating that the set of data that were stored has been altered, if the temporary signature is different than the signature.

13. The method of Claim 12, further comprising the step of sending the result from the server computing device to the client computing device so that the client device will apply the result to determine whether the set of data that were stored are usable by the client device.

14. The method of Claim 12, further comprising the step of determining if the signer ID that was received from the client computing device is on a list of banned signer IDs, and if so, indicating in the result that the set of data are not usable by the client computing device.

15. The method of Claim 5, wherein the key is a private key of a private key and public key pair, further comprising the steps of:

(a) computing the signature on the server computing device by signing the digest using the private key; and

(b) sending the signature to the client computing device for storage on the persistent storage.

16. The method of Claim 5, wherein the key is a private key of a private key and public key pair, further comprising the steps of:

(a) obtaining a signer identification (ID) for the client computing device, the signer ID uniquely indicating the client computing device and not being controlled by an operator of the client computing device;

(b) concatenating the signer ID with the digest before computing the signature on the server computing device by signing the signer ID concatenated with the digest using the private key; and

(c) sending the signature to the client computing device for storage on the persistent storage.

17. The method of Claim 16, wherein the step of verifying comprises the steps of:

(a) computing a temporary digest of the data that were stored in the persistent storage of the client computing device;

(b) using the public key of the private key and public key pair, using the client computing device to verify the signature that was stored, thereby recovering the digest and the signer ID; and

(c) comparing the temporary digest to the digest that was recovered to determine if the data that have been stored have been altered.

18. The method of Claim 17, further comprising the step of determining if the public key is still valid.

19. A memory medium on which machine readable instructions are stored for carrying out the steps of Claim 1.

20. A client computing device in which data are stored, comprising:

(a) a memory in which machine instructions are stored;

(b) a persistent storage used to store data;

(c) a network interface adapted to link the client computing device in communication with a server computing device over a network; and

(d) a processor coupled to the memory, the persistent storage, and the network interface, said processor executing the machine instructions to carryout a plurality of functions, including:

(i) before storing data, obtaining a signature for the data determined using a key known only by a server computing device and not available to the client computing device;

(ii) storing the data and the signature in the persistent storage;

(iii) before using the data that were stored in the persistent storage, obtaining a verification that the data have not been altered as a function of the signature; and

(iv) only using the data that were stored if the step of obtaining the verification indicates that the data that were stored have not been changed since the signature was computed before storing the data and the signature.

21. The client computing device of Claim 20, wherein the machine instructions further cause the processor to compute a digest of the data before the data are stored in the persistent storage, said digest being sent to a server computing device for computing the signature.

22. The client computing device of Claim 21, wherein the machine instructions further cause the processor to store a signer identification (ID) that is used in computing the signature, the signer ID uniquely identifying the client computing device and being uncontrolled by the client computing device or an operator of the client computing device, so that the signature establishes a relationship between the data before the data are stored and the signer ID.

23. The client computing device of Claim 20, wherein the data comprises a plurality of sets of data, and wherein the machine instructions further cause the processor to:

(a) request an intermediate key from a server computing device for use in computing a signature of each set of the data before the set is stored in the persistent storage, the intermediate key being determined as a function of a signer identification (ID) and an arbitrary value, the signer ID uniquely identifying the client computing device and being uncontrolled by the client computing device or an operator of the client computing device, said client computing device receiving the intermediate key, the arbitrary value, and the signer ID;

(b) computing a digest of each set of the data;

(c) computing the signature of the digest for each set of the data using the intermediate key; and

(d) storing the signature, the arbitrary value, and the signer ID in the persistent storage.

24. The client computing device of Claim 23, wherein before using the data that were stored, the machine instructions further cause the processor to compute a temporary digest of the data that were stored; and then send the temporary digest, and the signature, the arbitrary value, and the signer ID that were stored to a server computing device for verification that the data and the signer ID have not been changed.

25. The client computing device of Claim 20, wherein a private key and public key are used for signing and verifying the data, and wherein before storing the data, the machine instructions further cause the processor to compute a digest of the data that were stored, and then send the digest of the data to a server computing device for signing with the private key, so that the signature of the digest can be returned to the client computing device for storage with the data.

26. The client computing device of Claim 25, wherein before using the data that were stored, the machine instructions further cause the processor to:

(a) compute a temporary digest of the data that were stored;

(b) use the public key to verify the signature and thereby recover the digest; and

(c) determine whether the temporary digest is the same as the digest that was recovered to confirm whether the data that were stored have been altered, and thus, to determine whether to use the data that had been stored.

27. A server computing device that is employed in determining whether data stored in a persistent storage on a client computing device have been altered since the data were initially stored, comprising:

(a) a memory in which machine instructions are stored;

(b) a network interface adapted to link the server computing device in communication with a client computing device over a network;

(c) a processor coupled to the memory, and the network interface, said processor executing the machine instructions to carryout a plurality of functions, including:

(i) employing a key that is only known and available for use by the server computing device to compute a signature for the data before the data are stored in a persistent storage by a client computing device, said signature being sent to a client computing device and stored in a persistent storage in association with the data; and

(ii) before the data that were stored are subsequently used by a client computing device, facilitating a verification that the data that were stored have not been altered.

28. The server computing device of Claim 27, wherein the machine instructions further cause the processor to sent a result of the verification to the client computing device.

29. The server computing device of Claim 27, wherein the machine instructions further cause the processor to compute the signature based upon a digest of the data that is to be stored, where the digest is received from a client computing device.

30. The server computing device of Claim 27, wherein the machine instructions further cause the processor to use the key in determining the signature from a concatenation of a digest of the data that is to be stored and a signer identification (ID) uniquely identifying a client computing device on which the data are to be stored, wherein the signer ID is uncontrolled and unalterable by the client computing device and an operator of the client computing device, the signer ID being sent by the server computing device to the client computing device with the signature.

31. The server computing device of Claim 30, wherein the machine instructions further cause the processor to receive a temporary digest of the data that had been stored on a client computing device and the signer ID that had been stored on the client computing device, and compute a temporary signature of a concatenation of the signer ID and the temporary digest using the key, and then to verify whether the data or the signer ID that were stored were altered, by comparing the temporary signature with the signature, before sending a result of the comparison to the client computing device.

32. The server computing device of Claim 27, wherein the machine instructions further cause the processor to respond to a request for an intermediate key from a client computing device by computing the intermediate key from an arbitrary value and a signer identification (ID) uniquely identifying the client computing device, wherein the signer ID is uncontrolled and unalterable by the client computing device and an operator of the client computing device, the server computing device then sending the intermediate key, the arbitrary value, and the signer ID to the client computing device to enable the client computing device to store the arbitrary value, and the signer ID and to use the intermediate key to sign each of a plurality of sets of the data before storing the sets of the data.

33. The server computing device of Claim 32, wherein the machine instructions further cause the processor to:

(a) receive a temporary digest of a set of data that had been stored, along with the signature, the arbitrary value, and the signer ID that were stored;

(b) compute a temporary intermediate key by using the key to sign the signer ID and the arbitrary value that were received;

(c) compute a temporary signature for the set of data using an intermediate key;

(d) compare the temporary signature and the signature to verify whether the set of data or the signer ID that have been stored have been altered; and

(e) sending a result of the comparison to the client computing device.

34. The server computing device of Claim 27, wherein the key comprises a private key of a private and public key pair, and wherein the machine instructions further cause the processor to:

(a) receive a digest of the data that are to be stored from a client computing device; and

(b) compute the signature by using the private key to sign the digest.

35. The server computing device of Claim 27, wherein the key comprises a private key of a private and public key pair, and wherein the machine instructions further cause the processor to:

(a) receive a digest of the data that are to be stored from a client computing device; and

(b) compute the signature by using the private key to sign a concatenation of the digest and a signer ID uniquely identifying the client computing device, the signer ID being uncontrolled and unalterable by the client computing device and an operator of the client computing device.

36. The server computing device of Claim 34, wherein before a client computing device uses the data that were stored, the machine instructions further cause the processor to send a list of valid public keys to the client computing device to confirm that the private key used to sign the digest has not been made public.